

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

**IN THE MATTER OF THE CRIMINAL
COMPLAINT AND APPLICATION
FOR WARRANTS AUTHORIZING
THE SEARCH OF THE
PERSON, PREMISES, AND
ACCOUNTS IDENTIFIED IN
ATTACHMENTS A1-A5**

Case No. 1:21-mj-2820 to -2825 TMD

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR
SEARCH WARRANTS AND CRIMINAL COMPLAINT**

I, Brian Maddox, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Department of Veteran Affairs (VA), Office of Inspector General (OIG) and have been so employed since May 2020. Prior to employment with VA OIG, I was previously employed with the United States Department of the Army from May 2010 to May 2020, focused on national security investigations and strategic counterintelligence operations. Your affiant is a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Glynco, Georgia. I have also received additional training and have experience in criminal investigations. I have a Bachelor of Sciences Degree from the United States Military Academy at West Point.

2. I am currently assigned to the VA OIG Mid-Atlantic Field Office, Washington, District of Columbia (DC). As such, part of my duties include investigating crimes committed against programs and operations of VA by employees and non-employees, as well as allegations of serious violations of policies and procedures by high-ranking members at VA. These duties also include investigating matters related to persons who knowingly and willingly commit fraud against the United States.

3. The statements in this affidavit are based on my personal knowledge and observations during the course of this investigation; information observed by or known to other law enforcement officials that they conveyed to me; my personal review of records, documents, and other evidence obtained during the investigation; and information gained through my training and experience.

4. This affidavit is intended to show sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

PURPOSE OF THE WARRANTS

5. I make this affidavit in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to search and examine the following:

a. Facebook Account: Records and information associated with the account, further described in Attachment A1, that is stored at the premises owned, maintained, controlled, or operated by Facebook, Inc., a business with headquarters at 1601 Willow Road, Menlo Park, CA 94021:

<https://www.facebook.com/HISROYALFINEST>

b. Instagram Account: Records and information associated with the account, further described in Attachment A2, that is stored at the premises owned, maintained, controlled, or operated by Facebook, Inc., a business with headquarters at 1601 Willow Road, Menlo Park, CA 94021: **https://instagram.com/aik_swoo/; User ID: aik_swoo.**

c. Twitter Account: Records and information associated with the account, further described in Attachment A3, that is stored at the premises owned, maintained, controlled, or operated by Twitter, Inc., a business with headquarters at 1355

Market St, Ste 900, San Francisco, California 94103:

<https://twitter.com/WILLIAMRICH2004>; User ID: WILLIAMRICH2004.

d. Subject Premises: SUBJECT PREMISES, further described in Attachment A4, is a house located at 3114 Buds Circle, Windsor Mill, Maryland. Your affiant knows the William RICH resides at this location from a review of financial records, public records from the Maryland Department of Assessments and Taxation, VA records, and from law enforcement surveillance. Your Affiant seeks the authority to search the premises, including any vehicles or structures located thereon, as well as any electronic devices reasonably believed to be those of RICH or to contain depictions of RICH, for the evidence described in Attachment B4.

e. Persons and electronic devices: Finally, Your Affiant seeks to search the person and electronic devices found thereon of William Rich, further described in Attachment A5, for the evidence described in Attachment B4.

6. Your Affiant seeks this information in order to locate and seize evidence of violations of 18 U.S.C. §§ 641 and 1343 (theft of government property and wire fraud, respectively), (the “Subject Offenses”).

7. I further make this affidavit in support of an application for a criminal complaint and arrest warrant for William Rich, further described in Attachment 1 for violation of 18 U.S.C. §§ 641 and 1343 (theft of government property and wire fraud, respectively).

JURISDICTION

8. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

FACEBOOK

9. Facebook is a free social networking website that provides a host of services to its users. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. Facebook users can post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user’s profile page includes a “Timeline,” which is a space where the user and his or her “Friends” can post messages, attachments, and links.

10. Facebook has a Photos application, where users can upload images and videos. Another feature of the Photos application is the ability to “tag” (i.e., label) other Facebook users in a photo or video. For Facebook’s purposes, a user’s “Photoprint” includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

11. Facebook users can exchange private messages with one another. These messages, which are similar to email messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

INSTAGRAM

12. Instagram is an online mobile photo-sharing, video-sharing, and social networking service that enables its users to take pictures and videos, and share them either publicly or privately on the app, as well as through a variety of other social networking platforms, such as Facebook,

Twitter, Tumblr, and Flickr. Instagram has no set limit on the amount of data a user uploads to Instagram.

TWITTER

13. Twitter is an online social networking service that enables users to send and read short messages called “Tweets.” Users can send text messages, or use Twitter to share pictures, and videos. Twitter allows users to communicate directly and privately, enabling them to share text communications and media files.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. As described above and in Attachment B4, this application seeks permission to search for records that might be found on certain persons, premises, and in vehicles in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrants sought would authorize the seizure of electronic storage media found on said persons, premises and in said vehicles, or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

VA DISABILITY COMPENSATION PAYMENTS

15. The VA administers the the Disability Compensation program, a tax-free monetary benefit paid to veterans with disabilities that are the result of a disease or injury incurred or aggravated during active military service. The VA rates the level of service-connected disability of veterans on a scale of 0% to 100%. In calculating the rating, the VA considers the average detriment to a veteran’s earning capacity caused by each disability a veteran claims. The amount of disability compensation a veteran received is commensurate with their service-connected disability rating.

16. The VA also operates the Caregiver Assistance Program which pays a monthly stipend to family members who reside with and serve as caregivers to veterans who suffered serious injuries related to their active-duty service, and who need personal care because they cannot perform everyday activities.

17. The VA also administers the Special Monthly Compensation (SMC) program, which pays higher rate of disability compensation to qualifying veterans due to special circumstances such as the need of aid and attendance by another person for a specific disability, such as loss of use of legs.

18. Benefit payments are made monthly, and travel over interstate wires. In this case, payments typically originated from the VA's "Corporate Database" located in Austin, Texas, and traveled through entities in other states, including frequently the Department of the Treasury Disbursing Office located Kansas City, Missouri, before being deposited to the account of William RICH at Wells Fargo Bank, located in Minneapolis, Minnesota.

PROBABLE CAUSE

19. Since 2018, VA OIG has investigated William RICH (DPOB: 08/04/1980 Baltimore, Maryland) for fraudulent disability compensation claims. During the investigation, VA OIG special agents discovered that RICH misrepresented his physical condition in VA disability compensation claims, in communication with VA, and during medical examinations RICH underwent in pursuit of VA disability compensation benefits. In short, RICH falsely claimed to the VA that he is paralyzed and unable to walk and as a result, received benefits including Disability Compensation, Special Monetary Compensation and Caregiver Assistance Compensation, as well as medical care and subsidies for medical equipment from the VA totaling over \$800,000 to which he was not entitled.

20. Since 2007, RICH has received VA disability compensation for injuries sustained on August 23, 2005, while he was enlisted with the United States Army (Army), in Baqubah, Iraq.

21. RICH's Certificate of Release or Discharge from Active Duty, DD Form 214 (DD214), states that he served in the Army from September 22, 1998 to February 27, 2007.

22. The VA rated RICH 100% disabled due to, among other things, "[l]oss of use of both lower extremities...", "[n]eurogenic bowel," and "[p]ost-traumatic stress disorder with short-term memory loss." RICH was also awarded Special Monthly Compensation "...on account of loss of use of a creative organ from 02/28/2007...paraplegia with loss of use of both legs and loss of anal and bladder sphincter control from 02/28/2007," and given allowances for a caregiver, "Automobile and Adaptive Equipment," and "Specially Adapted Housing."

23. I contacted Social Security Administration (SSA), OIG and it indicated that RICH was receiving monthly SSA Disability Insurance Benefit payments. SSA OIG indicated that SSA relied upon documentation it received from VA in support of RICH's SSA disability claim. SSA OIG stated that when an SSA disability benefits applicant is also a military veteran, SSA requests and receives medical records directly from VA to verify and support the applicant's claim of disability.

24. As the investigation is ongoing and remains covert, SSA has not yet made an administrative determination of whether RICH is entitled to Social Security Disability Insurance Benefit payments. However, thus far, SSA has paid RICH over \$240,000 in benefit payments to which he may not be entitled, based on the fraudulent information in his claim for VA benefits.

25. VA treatment records stored in RICH's Veterans Benefits Management System (VBMS) file, included a document entitled "SCI&D Annual History & Physical," dated October 7,

2005, that suggest that RICH recovered from his injuries. The records memorialized RICH's condition and medical history upon admission to VA's Spinal Cord Injury and Disorder Center, Richmond, Virginia. RICH's medical history stated, "...MRI on the 24th of August [2005] revealed no cord impingement, no cord abnormalities and possible cord infarct." The document also noted RICH's "...paralysis has resolved somewhat and at present he is able to move his lower extremities." Finally, the record stated that RICH was "...continent of bowel and bladder."

26. VA treatment records stored in RICH's VBMS file, included a document entitled "SCI&D Clinician Reported FIM" dated December 5, 2006, which memorialized an assessment of RICH's condition using Functional Independence Measures (FIM) by a Certified Rehabilitation Registered Nurse (CRRN). RICH's FIM indicated "complete independence" or "modified independence" for all measures, including but not limited to, "toileting," "bladder mgt," "bowel mgt," "transfers," and "locomotion."

27. However, later records dated October 12, 2007, which memorialized an exam conducted on October 11, 2007 stated, "Since his accident, he has been paralyzed in both lower extremities; has been confined to a wheelchair and has no control of bowel, or bladder." The examining physician noted that "[t]here is no objective evidence of pain on motion. The patient arrives in a wheelchair and cannot arise from. He cannot stand or ambulate even with maximal assistance." Records indicate the physician did not order X-rays to confirm RICH's apparent condition, because he "did not feel that it was worth the trauma to him of manipulating him around for x-ray." Further, the physician noted "The C file is not available," indicating that he did not have access to RICH's complete claims file to review RICH's medical history or observe the earlier, contradictory report. Based on this examination, RICH was granted permanent disability from VA.

28. In or about 2018, VA OIG conducted an audit of certain claims, and learned of conduct by RICH inconsistent with his purported condition. VA OIG opened an investigation into possible fraud in RICH's claim for VA benefits.

29. On March 28, 2019, VA OIG SAs conducted physical surveillance, beginning at VA Medical Center (VAMC) Baltimore, MD. On that date, RICH attended a medical appointment. He presented to the appointment in a wheelchair but immediately following the appointment, in the VAMC Baltimore parking garage, RICH placed his wheelchair in the trunk of his vehicle and walked to the driver's door of his vehicle. Later that same day, VA OIG SAs observed RICH visit a barber shop at 2327 N. Rolling Road, Windsor Mill, Maryland, and walk from his vehicle to the barber shop. VA OIG SAs also observed RICH standing inside the barber shop.

30. From December 19, 2019 until May 6, 2020, covert electronic surveillance captured footage of RICH walking, ascending and descending stairs, entering and exiting vehicles, lifting, bending, and carrying items. I observed RICH conduct these activities, almost daily during the period of recording, without visible limitation or assistance of a medical device. I did not observe RICH use a wheelchair for mobility at any time during the period of recording.

31. On January 13, 2020 at approximately 2:01pm, I observed RICH retrieve a wheelchair from the trunk of a sedan and push the wheelchair into his garage. On that same date, at approximately 11:00am, RICH attended a dental appointment at VAMC, Baltimore, likely in the wheelchair.

32. Likewise, on February 5, 2020, at approximately 2:44pm, I observed RICH lift a wheelchair from the trunk of a sedan and carry the wheelchair into his garage. On that same date, at approximately 1:00pm, RICH had attended a dental appointment VAMC Baltimore, where he again likely presented in the wheelchair.

33. On February 4, 2021, RICH called the VA National Call Center to inquire about a pending claim. All calls to the VA National Call Center are recorded. Before recording, callers are advised by a preamble that states, “please hold while we transfer your call; your call may be monitored or recorded to evaluate the quality of our service to you.” During the call, RICH stated, “I’m calling to find out why I have an open claim.” RICH explained to the VA operator that his disability was permanent and stated, “...I have been in a wheelchair since 2005.” The operator explained to RICH that his benefits may be reviewed at any time. The operator also asked RICH if he could “...walk at all...” or “...carry anything.” RICH asked what the VA operator meant, and the VA operator stated “...as in carry something up a flight of stairs or walk for a limited time.” RICH replied “no” to the VA operator.

34. The next day, agents observed RICH at 4201 Northview Drive, Bowie, Maryland, the location of the VA-contracted medical examination provider. RICH appeared unable to stand and unable to enter and exit a vehicle without assistance.

35. Records from that visit contained a statement by RICH, “I am in wheelchair because both of my feet a (sic) paralyzed.” The provider noted, “...Veteran was involved in an IED blast in 2005 while deployed to Iraq that injured his left kidney and he ended up with a left nephrectomy and neurogenic bladder. He also had a spinal cord injury that left him paraplegic. He has since been confined to a wheelchair.” RICH’s condition was described as “[p]araplegic, bilateral lower extremity pain” that has “[s]tayed the same over time.” Based on this examination, RICH’s VA benefits were continued without modification to his disability rating or resulting disability compensation.

36. On May 6, 2021, members of the investigative team conducted physical surveillance of RICH attending a medical appointment for routine care at VAMC Baltimore. As with other visits

to VA-related medical appointments, RICH used a wheelchair to move from his vehicle in the parking garage to his medical appointments and back to his vehicle.

37. On June 2, 2021, members of the investigative team conducted physical surveillance beginning in the area of RICH's residence. On that day, I observed RICH exit his vehicle and walk, without the assistance of a wheelchair, in the parking lot in vicinity of 7216 Windsor Mill Rd B, Windsor Mill, Maryland. I also observed RICH exit his vehicle and walk, without the assistance of a wheelchair, to the business located at 6669 Security Boulevard, Woodlawn, Maryland. In CCTV footage from the same location, on the same date, RICH appeared able to walk, sit and stand from a chair, and maintain a stable standing position without visual indication of a physical disability.

38. Throughout the course of all of my surveillance, the only time I observed RICH use a wheelchair was in connection with VA-related medical visits.

TARGET ACCOUNTS

39. I believe the Target Accounts are likely to contain evidence of the suspected criminal activity. In particular, stored communications related to the fraud, as well as communications concerning, and photographs and videos of RICH engaged in activities inconsistent with his claimed disabilities.

40. I have made observations of the public portion of the Facebook page accessible at <https://www.facebook.com/HISROYALFINEST>. That Facebook account has a profile photo depicts a black male who resembles the person I know to be RICH. Additionally, the username "HISROYALFINEST" is the same as a Yahoo, Inc. email account, HISROYALFINEST@Yahoo.com, which is known to be used by RICH. Limited content is available for viewing by any person, without a requirement to log in to Facebook or for the viewer to have a Facebook account. On November 1, 2018, and again on April 2, 2021, members of the

investigative team observed photographs on RICH's Facebook page that contained images of RICH in an upright standing position and with no visible indication that he was bound to a wheelchair. An image dated May 19, 2012, and uploaded to Facebook on May 23, 2012, appeared to show RICH in an upright position. Multiple images uploaded to Facebook on January 28, 2012 also appear to show RICH in an upright position.

41. The Instagram user "aik_swoo," which is accessible at https://www.instagram.com/aik_swoo/, has a profile photo depicts a black male who resembles the person I know to be RICH. I have made observations of the public portion of the Instagram account, "aik_swoo" that I believe is owned and used by RICH. Some content on that account is available for viewing by any person, without a requirement to login to Instagram or for the viewer to have an Instagram account. However, only a portion of RICH's Instagram page is publicly available. Examples of content which may provide evidence of fraud include posts on December 14, 2020, and again on April 2, 2021, which contain images of RICH in an upright position with no visible indication that he was bound to a wheelchair.

42. I have made additional observations of RICH's Instagram page through an Instagram replication and downloading website, "imginn.com." The content, which is a duplicate of existing Instagram pages, makes all Instagram content available for viewing and download by any person. RICH's Instagram content, through "imginn.com," is accessible at the following URL: https://imginn.com/aik_swoo/. The page contained multiple images of RICH beginning in 2014 and was updated as recently as February 2021. Two videos uploaded to RICH's Instagram page in December 2020, contain footage of RICH walking, bending, standing from a seated position, and participating in weightlifting exercises. A photograph uploaded to RICH's Instagram page in 2016 contained an image of RICH in a gym, dressed in athletic apparel, standing without visible

assistance. The same photograph contained the caption, “Lol lift or leave. The gym is now known as Gainesville aka LIFTUATION HQ.” A photograph uploaded to RICH’s Instagram page in 2014 contained an image of RICH standing in a crouched position without visible assistance.

43. I have made observations of the public portion of the Twitter account at <https://twitter.com/WILLIAMRICH2004>. That Twitter account has a profile photo depicts a black male who resembles the person I know to be RICH and further has a username “WILLIAMRICH2004.” Additionally, the username “WILLIAMRICH2004” is the same as a Yahoo, Inc. email account, WILLIAMRICH2004@Yahoo.com, which is known to be used by RICH. The content is available for viewing by any person, without a requirement to log in to Twitter or for the viewer to have a Twitter account. On December 14, 2020, and again on April 2, 2021, I observed photographs on RICH’s Twitter page that contained images of RICH in an upright standing position without visible assistance and no visible indication that he was bound to a wheelchair. RICH’s Twitter page contained posts beginning in 2014 and was uploaded as recently as March 1, 2021. A photograph of RICH, uploaded on May 20, 2017, contained an image of RICH standing in an upright position.

44. RICH listed email addresses, HISROYALFINEST@Yahoo.com and WILLIAMRICH2004@Yahoo.com on documents filed with the VA regarding disability compensation benefits. On October 17, 2005, RICH applied for VA disability compensation benefits and listed HISROYALFINEST@Yahoo.com among his contact information. On September 3, 2019, RICH submitted a document, to VA, regarding his dependents that listed WILLIAMRICH2004@Yahoo.com among his contact information.

45. Based on my training and experience, I know individuals who fraudulently claim medical conditions for the purpose of VA disability compensation often post information on

social media accounts that reveal their activities and physical condition. RICH's public social media profiles demonstrate that he stores information pertaining to his daily activities on his social media accounts including photographs, videos, and messages. That content includes examples of RICH's physical condition which appears to contradict the physical condition RICH reports to VA for the purpose of disability compensation benefits. As a result, RICH receives disability funds from the United States Government to which he is not entitled in violation of 18 U.S.C. §§ 641 and 1343, theft of government property and wire fraud, respectively.

Accordingly, there is probable cause to believe that additional evidence of this violation will be found in the non-public portions of the Target Accounts, such as messages, and additional photographs or videos.

THE SUBJECT PREMISES

46. I believe the Subject Premises is likely to contain evidence that RICH is not disabled as he purports to be. For example, I know from posts on the publicly viewable portion of his Instagram page that his home is likely to contain an extensive gym, with exercise equipment that a person in RICH's purported condition would not be capable of using.

47. While I am aware that RICH received reimbursement for the installation of a chair lift ramp in his home, I have not yet been able to verify whether the chair lift actually was installed. Moreover, the absence of equipment such as grab bars, ramps, a specialized bed, or specialized toileting and showering equipment will further serve to establish that RICH exaggerated and misrepresented his physical condition to the VA.

48. Finally, RICH received funds from the VA to purchase a specially adapted vehicle to accommodate his claimed disability. RICH was also trained by VA in the use of vehicle hand controls to safely operate an adapted vehicle. RICH used the funds in 2006 to

purchase a 2004 BMW 645ci, a 325 horsepower two-door luxury sports car, which, due to its limited dimensions, is not readily adaptable to the use of a paraplegic person.

49. Though RICH totaled the BMW in an accident, he currently owns and routinely operates two vehicles that he stores on the Subject Premises, a 2016 Chevrolet Suburban, and a 2009 BMW 750 which, based on surveillance of the vehicles in operation, do not appear to be equipped with hand controls or otherwise adapted for a person in RICH's purported condition. A search of these vehicles would confirm whether they are equipped such that a paraplegic person would be able to operate them.

ELECTRONIC DEVICES

50. Through my training and experience I know that individuals who commit fraud often document the spoils of their frauds through photographs captured on their phones and other camera-equipped electronic devices, and store them on those and other electronic devices. I believe that such electronic devices found on RICH's person and the Subject Premises are likely to contain photographs and communications relating to RICH's purchases made using the stolen funds, and will also depict RICH engaging in activities inconsistent with his purported disabilities.

51. In addition, I have observed hard-wired security cameras affixed to RICH's home. I believe that certain electronic devices within the home may contain stored recordings from the cameras that depict RICH engaging in activities inconsistent with his purported disabilities.

CONCLUSION

52. There is probable cause to believe that RICH committed violations of 18 U.S.C. §§ 641 and 1343 (theft of government property and wire fraud, respectively), and that evidence of that offenses may be found in the Target Accounts, Subject Premises, and on the person and

electronic devices of William RICH. I therefore that the Court issue the proposed search warrants and arrest warrant.

53. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the warrants for the Target Accounts. Because those warrants will be served on the named companies who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

REQUEST FOR SEALING

54. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

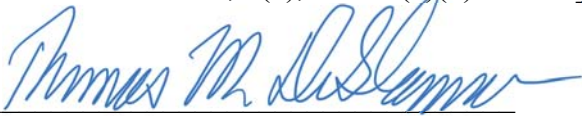
Respectfully submitted,

Brian J. Maddox
3491242

Digitally signed by Brian J.
Maddox 3491242
Date: 2021.10.11 09:28:49
-04'00'

Brian J. Maddox (Affiant)
Special Agent
Department of Veteran Affairs
Office of Inspector General

Affidavit submitted by email and attested to me as true and accurate by telephone pursuant to Fed. R. Crim. P. 4.1, 4(d), and 41(d)(3) on this 12 day of October 2021.



The Honorable Thomas M. DiGirolamo
United States Magistrate Judge

✓ FILED _____ ENTERED
_____ LOGGED _____ RECEIVED

1:21-mj-2820 to -2825 TMD

11:05 am, Oct 14 2021

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

ATTACHMENT A1 – Facebook, Inc.

This warrant applies to information associated with the Facebook account

“HISROYALFINEST” at <https://www.facebook.com/HISROYALFINEST>, that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a business headquartered at 1601 Willow Road, Menlo Park, CA 94025

✓
____ FILED ____ ENTERED
____ LOGGED ____ RECEIVED

1:21-mj-2820 to -2825 TMD

11:06 am, Oct 14 2021

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

ATTACHMENT A2 – Instagram, Inc.

This warrant applies to information associated with the Instagram account “aik_swoo” at https://www.instagram.com/aik_swoo/ that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc., and headquartered at 1601 Willow Rd, Menlo Park, CA 94025.

✓ FILED _____ ENTERED
_____ LOGGED _____ RECEIVED

11:06 am, Oct 14 2021

1:21-mj-2820 to -2825 TMD

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

ATTACHMENT A3 – Twitter, Inc.

This warrant applies to information associated with the Twitter account
“WILLIAMRICH2004” at <https://twitter.com/WILLIAMRICH2004> that is stored at the
premises owned, maintained, controlled, or operated by Twitter, Inc., a business with
headquarters at 1355 Market St, Ste 900, San Francisco, California 94103.

✓ FILED _____ ENTERED
LOGGED _____ RECEIVED

1:21-mj-2820 to -2825 TMD

11:06 am, Oct 14 2021

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

ATTACHMENT A4

Subject Premises

The house located at 3114 Buds Circle is a residence in Windsor Mill, Maryland, which is a white siding and partial stone-front modern colonial-style home. The residence has an attached two car garage, a detached shed, a basement, and is situated on a .2 acre lot. The house number “3114” is marked on the mailbox adjacent to the house’s driveway as well as on the door frame to the right of the front door. It is located within Baltimore County, Maryland.



✓ FILED ____ ENTERED
____ LOGGED ____ RECEIVED

11:06 am, Oct 14 2021

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

ATTACHMENT A5

Person to be Arrested and Searched

1. William Rasheem Jamal RICH, DOB: 08/04/1980, SSN: XXX-XX-9305.



ATTACHMENT B1 - Facebook, Inc.

I. Files and Accounts to be produced by Facebook, Inc. for the period August 23, 2005 to the present.

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Facebook including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Facebook or have been preserved pursuant to a preservation request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A1:

- a. Any and all associated subscriber information and user contact info, including, but not limited to, all “About Me” data, user identification number, current name and any prior names associated with the Target Account(s), alternate names, birth date, contact email addresses, including removed email addresses, physical addresses, associated or registered telephone numbers, associated screen names, associated websites, apps, registration date, and work data;
- b. A user “neo-print,” including account status history, profile contact information, date and time of account creation, historical login information, mini-feed, status update history, shares, notes, wall and timeline postings to the Target Account(s), wall and timeline postings made by the Target Account(s) to other accounts, friend listing, including deleted or removed friends and friends identified as “Family,” the names of all users listed as “Followers” or as “Following,” networks, groups listing, future and past events, and video listing;
- c. A user “photo-print,” including all undeleted or saved photos, photos in which the user has been “tagged” with the user name, and all associated metadata or EXIF data with any such photos;
- d. Any and all associated Groups information, including a list of all other users currently registered in any such groups and the current status of the group profile;
- e. Any and all public or private messages, including any attached documents, images, or photos, including from the Facebook Messenger app, the Facebook mobile app, and the Facebook website accessed via mobile device (including phone or tablet) or computer;
- f. All notes written and published to the Target Account(s);
- g. All Internet Protocol (“IP”) logs for the Target Account(s) from @@ to the present, including script data, script get data, user ID, view time, IP source information, login and logout data, and active sessions data;
- h. All chat history, including, but not limited to, the content of all chats and date and time information for all chats, including from the Facebook Messenger app, the Facebook mobile app, and the Facebook website accessed via mobile device (including phone or tablet) or computer;
- i. All check-in data;

- j. All Connections data, including, but not limited to, all users who have liked the Page or Place of the Target Account(s);
- k. All stored credit card numbers;
- l. All Events data;
- m. All Friend Requests data, including pending sent and received friend requests;
- n. All associated data that is “Hidden from News Feed,” including any friends, apps, or pages hidden from the News Feed;
- o. The last location associated with an update;
- p. All “Likes on Other’s Posts,” “Likes on Your Posts from others,” and “Likes on Other Sites” data;
- q. A list of all linked accounts;
- r. A list of all “Pages You Admin” for the accounts listed below;
- s. All Physical Tokens data;
- t. All Pokes data;
- u. All Recent Activities data;
- v. All Searches data;
- w. All Shares data;
- x. All videos posted to the Target Account(s);
- y. The subscriber's registration information provided at time of account creation, including IP address(es);
- z. The subscriber's service and account information, including any billing address(es) provided, billing records, telephone numbers, IP address (at each transaction), and complete transactional information;
- aa. The subscriber's email address(es) and/or any email address(es) relating to the subscriber;
- bb. The subscriber's records of session times and durations and any information relating to the session including, but not limited to, any temporarily assigned network address, Internet Protocol (IP) address, MAC address;
- cc. The subscriber's length of service (including start date) and types of services utilized and any information associated with that service such Internet Protocol (IP) address, MAC address, Caller ID, and Automatic Number Identification (ANI);
- dd. The subscriber's means and source of payment for any financial transactions (including any credit card or bank number);
- ee. IP addresses and location data for all posts, wall posts, comments, friend requests, all messages and electronic communications, photo uploads, likes, Messenger messages and file transfers, and machine cookie information; and
- ff. Interstitial Facebook, Facebook Messenger, and Instagram accounts linked to the Target Account(s) by usernames, e-mail addresses, SMS numbers, credit card numbers, bank account numbers.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the account described in Attachment A1 which is evidence, fruits, and instrumentalities of violations of theft of government property and wire fraud including:

- a. All records, information, documents or tangible materials regarding:
 1. Communication between the target account(s) and other coconspirators, known or unknown;
 2. Email accounts, user names, or profiles associated with other coconspirators, known or unknown;
 3. Schedules, plans, meetings, communications, or activities while traveling outside or inside the United States;
 4. Financial records, benefits, documents, or statements related to the use of government benefits;
 5. Photo, videos, or other media featuring RICH, their children, spouses, or parents;
 6. Steps taken by RICH, or any other coconspirators to conceal their scheme from law enforcement or government officials; and,
 7. Use of any fraudulent documentation to receive money or benefits.
- b. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;
- c. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
- d. Evidence of the times the account was used;
- e. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- f. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account; and,
- h. All "address books" or other lists of contacts.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose

those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B2 - Instagram, Inc.

I. Files and Accounts to be produced by Instagram, Inc. for the period August 23, 2005 to the present.

To the extent that the information described in Attachment A2 is within the possession, custody, or control of Instagram including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Instagram or have been preserved, Instagram is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

1. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

2. Subscriber information for all other accounts linked to the Target Accounts, including by email address, phone number, Instagram or third-party cookies and machine cookies, unique device identifiers, or any other means by which Instagram links accounts that appear to have a common user;

3. All information automatically recorded by Instagram from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Instagram website, all information searched for on the Instagram website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;

4. The types of services utilized by the user;

5. All files and records or other information stored by an individual using the account, including all images, videos, documents, communications and other files uploaded, downloaded or accessed using the Instagram service, including all available metadata concerning these files;

6. All records pertaining to communications between Instagram and any person regarding the account, including contacts with support services and records of actions taken;

7. All data and information associated with the personal page and/or profile page, including photographs, videos, audio files, lists of personal interests and preferences, including hashtags;

8. A complete list of all users who are followed by the accounts and a list of all users who are following the accounts, including every user name, user identification number, corresponding email address, physical address, and date the user joined Instagram;

9. All photos, videos, messages and other files to which the accounts have been added, tagged, or associated, including any hashtags or captions associated with each photo, a list of all

user who “liked” each photo, a list of each user who commented on each photo, and the substance of each comment regarding each photo;

10. All photos, videos, messages and other files posted, screen shot, sent, received, or stored by the accounts, including the contents of all posts and direct or private messages, including any metadata, geotags, hashtags, captions, or comments associated with the content, a list of all users who “liked” or commented on each photo, video, or post, the usernames of any other user added to or tagged in each photo, video, comments;

11. All location data associated with the account;

12. All data and information that has been deleted or marked for deletion by the user;

II. Information to be seized by Law Enforcement Personnel

Any and all records that relate in any way to the account(s) described in Attachment A2 which is evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 641 and 1343, specifically that relate to the following:

- a. All records or other information;
- b. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;
- c. Communication, information, documentation and records relating to who created, used, or communicated with the account(s) or identifier(s), including records about their identities and whereabouts;
- d. Evidence of the times the account(s) or identifier(s) listed in Attachment A2 were used;
- e. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- f. Passwords and encryption keys, and other access information that may be necessary to access the account(s) or identifier(s) and other associated accounts;
- g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account(s);

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B3 - Twitter, Inc.

I. Files and Accounts to be produced by Twitter, Inc. for the period August 23, 2005 to the present.

To the extent that the information described in Attachment A3 is within the possession, custody, or control of Twitter, including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Twitter or have been preserved pursuant to a preservation request, under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account or identifier listed in Attachment A3:

- a. The contents of all of the user's public and private tweets, retweets, direct messages, profile photos, header photos, background images, locations, URLs, "bios," stored files (including videos, images and other files);
- b. All transactional information of all activity associated with the account, including usage information, log information, device information, information collected by cookies and other tracking technologies, third party cookies, page visits, communications with the Twitter support team, site registrations, log files, dates, times, methods of connecting, devices or software used, ports, dial ups, and/or locations;
- c. All records related to the devices, operating system, browser and cookies of the user;
- d. All records or other information stored by or associated with the user of the account, including lists of users who follow the subject user, users followed by the subject user, retweets, likes and notes;
- e. All records or other information regarding the identification of the account, to include application, full name, picture, email address, payment details, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;
- f. All search history or web history;
- g. All records indicating the services available to subscribers of the account;
- h. All usernames associated with or sharing a login IP address or browser cookie with the account;

- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user;
- k. All telephone or instrument numbers associated with the Target Account (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”));

II. Information to be Seized by the Government

Any and all records that relate in any way to the account(s) described in Attachment A3 that is evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 641 and 1343, specifically that relate to the following:

- h. All records or other information;
- i. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;
- j. Communication, information, documentation and records relating to who created, used, or communicated with the account(s) or identifier(s), including records about their identities and whereabouts;
- k. Evidence of the times the account(s) or identifier(s) listed in Attachment A3 were used;
- l. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- m. Passwords and encryption keys, and other access information that may be necessary to access the account(s) or identifier(s) and other associated accounts;
- n. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account(s);

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further

order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

ATTACHMENT B4

The Items to be Seized

Premises, Vehicles and Persons

- 1) All records relating to violations of 18 U.S.C. §§ 641 and 1343 including:
 - a. Records and information relating to a scheme to defraud government benefit programs;
 - b. Records and information relating to government benefit programs;
 - c. Records and information relating to the physical or medical condition of the suspect;
 - d. Photographs and videos of the suspect;
 - e. Bank and financial records, checks, money orders, traveler's checks, and domestic and international account numbers;
 - f. Records, documents, data, equipment, and materials related to adaptation of the Target Residence or Target Vehicle for handicap accessibility or use by a disabled person;
 - g. Medical equipment, prosthetics, assistance devices;
 - h. Health or fitness equipment and electronic health or fitness devices;
 - i. Documents, data, and materials that contain other peoples' personal identifiers that may relate to the Subject Offenses;
 - j. Keys for safes, safety deposit boxes, storage lockers, private mail boxes and post office boxes, and documents indicating the rental or ownership of such, that could potentially house the items that are authorized to be seized and records that may indicate the location or existence of such items or places.
- 2) Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified criminal offenses. The following definitions apply to the terms as set out in this affidavit and attachment:

- a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
- b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
- d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touches. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

3) For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a) evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b) evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c) evidence of the lack of such malicious software;
- d) evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e) evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f) evidence of the times the COMPUTER was used;
- g) passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h) documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i) contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
3. “scanning” storage areas to discover and possibly recover recently deleted files;
4. “scanning” storage areas for deliberately hidden files; or
5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.
6. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.